Refine Search

Search Results -

Terms	Documents
L9 and 705/39	33

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search:

Refine Search

Recall Text | Clear | Interrupt

Search History

DATE: Wednesday, June 21, 2006 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L10	L9 and 705/39	33	L10
L9	L8 and offer	318	L9
L8	L6 and (modify or modification or change or modif$)near account	422	L8
L7	L6 and (modify or modification or change or modif$) account	634702	L7
L6	L5 and payment	5044	L6
L5	l1 and (credit or debit) near account	6485	L5
L4	L3 and 705/39	29	L4
L3	L2 and (deposit and demand or escrow near2 account or required near2 deposit)	312	L3
L2	L1 and account near2 management	3210	L2
L1	(internet or web or www or network)	1834734	L1

END OF SEARCH HISTORY

Refine Search

Search Results -

Terms	Documents
L17 and 705/39	33

Database: US Pre-Grant Publication Full-Text Database; US Patents Full-Text Database; US OCR Full-Text Database; EPO Abstracts Database; JPO Abstracts Database; Derwent World Patents Index; IBM Technical Disclosure Bulletins

Search:

Refine Search | Recall Text | Clear | Interrupt

Search History

DATE: Wednesday, June 21, 2006 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L18	L17 and 705/39	33	L18
L17	L16 and offer	318	L17
L16	L15 and (modify or modification or change or modifi$) near account	422	L16
L15	L14 and payment	5044	L15
L14	l1 and (credit or debit) near account	6485	L14
L13	L7 and (modify or modification or change or modifi$) near payment near account	6	L13
L12	L7 and (modify or modification or change or modifi$) near payment adj account	6	L12
L11	L8 and 705/39	11	L11
L10	L9 and 705/39	10	L10
L9	L8 and offer	95	L9
	L7 and (modify or modification or change or modifi$) near payment		

L8	and account	116	L8
L7	l3 and (credit or debit) near account	6485	L7
L6	L5 and 705/39	29	L6
L5	L4 and account near2 management	312	L5
L4	L3 and (deposit and demand or escrow near2 account or required near2 deposit)	11644	L4
L3	(internet or web or www or network)	1834734	L3
L2	(internet or web or www or network)	1834734	L2
L1	(internet or web or www or network)	1834734	L1

END OF SEARCH HISTORY

L10: Entry 9 of 10 File: USPT Feb 16, 1999

DOCUMENT-IDENTIFIER: US 5872844 A
TITLE: System and method for detecting fraudulent expenditure of transferable electronic assets

Brief Summary Text (11):
Another proposed solution to double spending is to develop an online banking system to discover assets which have been double spent. In this system, each electronic asset that is spent is collected by a central bank or other institution and evaluated for possible double expenditure. Since the asset is non-transferable and can be spent only once, the discovery of identical assets reveals that the asset has been double spent. When a recipient receives a new asset, it uses the online banking network to determine whether that same asset has been previously spent. The primary drawbacks of the online approach are the high expense involved in managing an online system and the potentially long delay periods experienced when a recipient is attempting to verify a new asset. In addition, for the very large data bases required here, the current cost per transaction is too high for sub $1 transactions; hence, batching deposits into aggregates of total value $100, as proposed here, make it cost-effective. Another drawback is that not all recipients are online with the bank. For instance, the assets might be used in off-line devices, such as vending machines or toll booths. Networking all possible recipient machines would be extremely expensive.

Brief Summary Text (12):
A variation of the online bank system is for the bank to offer "after the fact" exposure of double spenders, which is particularly used in anonymous electronic asset systems. In this scenario, the bank evaluates each spent asset for possible double spending. As long as the user follows the stipulated guidelines and spends each asset only once, the user remains anonymous. However, if the user multi-spends the same asset, the bank detects the fraud and has enough information to identify the criminal user. Those culprits are then sought out and prosecuted.

Brief Summary Text (22):
The electronic asset system further includes a fraud detection system which samples a subset of the assets transferred from the payer wallets to the payee wallets. Each transferred asset is subject to being audited, with an exemplary sample rate being one in every 100 assets. The payee wallets are equipped with transmitters to send the transferred assets over a network, such as the Internet, to the fraud detection system.

Brief Summary Text (24):
Upon detection, the fraud detection system identifies the payer wallets that transferred the bad assets and marks the payer wallets as "bad." The fraud detection system then compiles a list of bad wallets and posts the list to warn other wallets. The list (which is also referred to as a "hot list" or "revocation list") is broadcast to the electronic wallets over a data communication network, such as a public network (e.g., the Internet) or a wireless network (e.g., cellular phone and paging network). The wallets are equipped with receivers to receive the broadcast transmission of the list. The entire list can also be posted to a central location (e.g., an Internet web site) so that anybody can access and download it.

Detailed Description Text (5):
The issuer and each party possesses tamper-resistant hardware/software devices. Communication channels 26(1)-26(6) facilitate communication among the issuer/collector 22 and the parties 24(1)-24(5). The channels are representative of many different types of connections, including direct local connections or remote connections over a communication network, such as a public network (e.g., the Internet, telephone, cable TV, etc.) or a wireless network (e.g., cellular phone, paging network, satellite, etc.). These channels are secured using cryptography protocol. More specifically, the communication between participants can be accomplished using secure channel protocols as well as secure messaging protocols.

Detailed Description Text (7):
The issuer 22 issues transferable assets to the first party P.sub.0 24(1). This issuance represents many different types of transactions. For example, the issuer 22 might be a bank and the first party 24(1) might be an account holder who is withdrawing assets from his/her account. A bank withdrawal transaction can be conducted over an online network connection 26(1), such as over a private banking network connection (e.g., ATM--automatic teller machine), or over a public network connection (e.g., the Internet) using commercial banking programs like Money from Microsoft Corporation. In another example, the issuer 22 might be a public transit authority, and the party 24(1) might be a citizen who purchases tokens to ride on the public transportation system. In this case, the network connection 26(1) might be established at an off-line point-of-sale vending machine that issues tokens to the user's electronic transit card.

Detailed Description Text (11):
According to the stick minting process, the withdrawing party P.sub.0 requests a stick of assets of size L. For instance, the party P.sub.0 might request a stick of one hundred $1 coins. Assuming the party P.sub.0 has the appropriate balance or credit in their account, the issuer 22 creates a stick of size L. To produce this stick, the issuer 22 selects the asset-related data X and runs it through a one-way function L times. One suitable one way function is SHA. Let h.sup.i (x) denote i application of the hash function h(), for i=1, 2, . . . , L. The result of the last hash operation, designated as variable y so that y=h.sup.L (x) is concatenated with the identification of the withdrawing party's P.sub.0 and digitally signed by the issuer to produce the issuer's signature, as follows:

Detailed Description Text (13):
Individual assets may be transferred a number of times, designated by a variable "k," before the assets are exhausted. As an example, each asset might be capable of being handed off ten times, for k=10. The number of permitted transfers can be established as a parameter for the entire electronic asset system, whereby a system that allows transferability of assets through k hands is called a "k-off" system. Every wallet that is capable of receiving and transferring assets in the k-off system is referred to as a "k-off" wallet. A k-off electronic wallet is a tamper-resistant device that is small and preferably portable. The k-off electronic wallet has memory to store the assets and cryptographic capabilities to store and manage public/private signing/encryption keys and certificates. The k-off electronic wallet is also equipped with a transmitter to communicate data over a network (e.g., Internet, cellular, RF, etc.) and a receiver to receive data over the same or a different network. The receiver is preferably a pager receiver for receiving messages from the fraud detection unit. The k-off electronic wallet can be implemented as a portable device with its own trusted display and keyboard, such as a hand held computer, a personal digital assistant, or a laptop computer.

Detailed Description Text (19):
During each transaction between a payer and payee, a payer spends or uses an asset in some manner by transferring the asset to the payee. For example, the payer might be a consumer and the payee might be a merchant, with the purchase occurring over a public network connection. In another example, the payer might be a thirsty

individual and the payee might be a beverage vending machine, with the communication link being an off-line direct connection at the vending machine. Still another example is for the payer to be one business entity and the payee to be another business entity.

Detailed Description Text (30):
The fraud detection unit 28 compiles a list of tainted or bad wallets. The list is distributed to the wallets of all the parties 24(1)-24(5) to warn other parties of the bad wallets. The list can be distributed from the fraud detection unit 28 to the wallets 24(1)-24(5) in a number of different ways. The list might be broadcast over a data communications network (i.e., Internet, interactive television, telephone, cable TV, etc.) or a wireless communications network (e.g., cellular, paging, radio, etc.). The list might be posted at a publicly accessible location, such as a web site. Alternatively, the list might be transported or mailed on a storage medium. The list is routinely updated as subsequent bad wallets are identified. Updates to the list are preferably broadcast in periodic intervals (e.g., every five seconds) to ensure that the parties receiving assets are kept current.

Detailed Description Text (37):
The electronic asset system 20 is beneficial at reducing connectivity and online requirements, as well as the transactions costs typically associated with full online verification systems. For small transactions where the asset value is low (e.g., coins, tokens), continuous online connection to a banking or merchant system on a per transaction basis is too expensive. For instance, it is impractical to expect a beverage vending machine to validate each beverage purchase over a network with a localized vending hub computer. Even if the transaction cost was sufficiently low, the real time response delay would be too long and annoying to the consumer, who simply wants a beverage for 75 cents.

Detailed Description Text (38):
With the early warning fraud detection unit, however, only a few samples are required, not every transaction. The samples can be provided over a limited online connectivity (e.g., via the Internet), or in the case of a standalone machine, in a periodic batch effort. Upon compilation of bad wallet lists, the fraud detection unit 28 can transmit updated lists in real time; or for the standalone machine, the list is updated upon routine collection rounds. The volume of online communication is a few orders of magnitude smaller than a full online system and involves reasonably tolerant response delays.

Detailed Description Text (43):
During certification, the electronic wallet 58 is connected to the bank's computer 62. This connection can be achieved, for example, using a direct connection, or alternatively over a public network (e.g., the Internet).

Detailed Description Text (49):
The coins, or stick of coins, are downloaded to the electronic wallets 56, 58 over respective secure communication channel 70, 68. The bank debits the user's account for the amount of money withdrawn. The coins are stored in the electronic wallets 56, 58. The user is free to carry the electronic wallet and use it wherever he/she wishes.

Detailed Description Text (62):
As part of the probabilistic fraud detection scheme, the k-off wallets 58, 72, and 76 periodically submit the received coins over a network 86, such as a public network like the Internet, to a fraud detection center (FDC) 90. The communication channels through the network 86 are secured. Additionally, other forms of networks may be used, such as telephone, RF, cable, and the like.

Detailed Description Text (63):

The coins are submitted in response to a routine audit request that is periodically broadcast by the fraud detection center 90. More particularly, the FDC computer broadcasts an unforgeable random number "r" in periodic intervals (e.g., every five seconds) over a network to the k-off electronic wallets 58, 72, and 76. The broadcast transmission can be conducted over the same network 86 as the coins were received, or over a separate network, such as a wireless network represented by RF tower 98. Preferably, the wireless network is implemented as a paging network which permits convenient and reliable downlinking of data from the FDC to the payee wallets. Other types of distribution networks may also be used, such as cable TV or interactive television systems, cellular phone, telephone lines, satellite systems, and the like.

Detailed Description Text (67):
The coin analysis might reveal multiple bad wallets. Accordingly, the FDC computer 92 compiles a list 96 in an electronically readable data structure that contains all of the bad wallets (step 164 in FIG. 5), or more specifically, all of the certificates of the bad wallets. The FDC computer 92 then broadcasts the updates to the list of bad wallets over the network 86 or wireless network 98 (step 166 in FIG. 5). Additionally, the entire list 96 can also be posted at a publicly accessible location for anybody to access and download, such as an Internet web site. The list is also sent to the bank 52 via a secure communication channel 100.

Detailed Description Text (69):
The k-off wallets 58, 72, and 76 are equipped with an appropriate receiver to receive the list 96 from the fraud detection center 90 as well as the audit command, r. The receivers might be an RF receiver to receive radio, cellular, and paging signals; or a network card to receive data over a network; or a modem to receive data over a phone line; or a satellite receiver to receive satellite packets. The local hot lists provide the k-off wallets with ready, on-the-spot identification of bad wallets. Any transaction that was delayed typically one audit interval is permitted to conclude if the audit results are positive.

Detailed Description Text (87):
Accordingly, to ensure true anonymity, the electronic asset system 50 enables the users 54 to break at will any linkability between withdrawal and payment, and between different payments, so that the transactions cannot be traced to the user. Breaking linkability is provided through the issuance of payment certificate(s) and separate withdrawal certificate(s) and the ability for the electronic wallet to change its payment certificate anonymously whenever the users 54 decide. None of the payment certificates are linkable to each other, nor to the withdrawal certificates. In this manner, the user can withdraw coins using one wallet certificate and identification, and then pay with another wallet certificate which can be changed at will.

Detailed Description Text (95):
With reference to FIG. 3, the wallet 76 is shown withdrawing assets with the bank 52. The k-off wallet 76 establishes a secure channel 78 with the bank's computer 62 and submits candidate coins and specifies their desired value and expiration dates. The bank assigns the value by choosing a signature exponent corresponding to that value. In the case of withdrawal, the authorized value equals the desired value if the user has sufficient funding in his/her account. The bank's computer blindly signs the coins and return them to the electronic wallet 58. If unused before the expiration date, the unexpired coin is refreshed by submitting it in exchange for a new coin of equal value with a new expiration date.

Detailed Description Text (111):
The above disclosure centered on an electronic asset system. However, it is noted that some aspects of this invention can be used generally in a public key cryptography system. In the more general case, electronic devices are assigned certificates with public and private key pairs. The devices then engage in

transactions according to a set of prescribed rules which typically involves digital signing using the private signing key. This certificate is marked as revoked. The sample and detection system then compiles a list of revoked certificates which is broadcast to all of the payee electronic devices over a paging network, or the like. By using short expirations and storing short hashes of the revoked certificates, the list is short enough to be stored locally on the electronic devices. These local lists are then used to prevent further perpetuation of non-compliance with the rules.

Issued US Cross Reference Classification (3):
705/39

Field of Search Class/SubClass (4):
705/39

CLAIMS:

8. An electronic asset system as recited in claim 1, wherein the electronic wallets comprise a transmitter to transmit the transferred electronic assets over a network to the fraud detection system.

12. An electronic asset system as recited in claim 9, wherein the fraud detection system transmits the list over a network.

21. An early detection and warning system as recited in claim 18, further comprising a network connection to an electronic data network, the computer being further programmed to transmit an identity of the bad wallet via the network connection over the electronic data network.

22. An early detection and warning system as recited in claim 18, further comprising a transmitter to broadcast an identity of the bad wallet over a broadcast communication network.

36. An electronic asset system as recited in claim 32, wherein:

the fraud sampling unit transmits the list of the bad payer asset holders over a network; and

the payee asset holders are equipped with a receiver to receive the transmitted list.

37. An electronic asset system as recited in claim 32, wherein the fraud sampling unit broadcasts the list of the bad assets holders over a data communications network selected from a group comprising a wire-based public network, a cable-based entertainment network, and a wireless communications network.

Previous Doc Next Doc Go to Doc#

Refine Search

Search Results -

Terms	Documents
L12 and (request or asks or insist or message) and cancel and account	16

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search:

Refine Search

Recall Text

Clear

Interrupt

Search History

DATE: Wednesday, June 21, 2006 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR		
L14	L12 and (request or asks or insist or message) and cancel and account	16	L14
L13	L12 and request and cancel and account	16	L13
L12	L11 and (dissatisfied or dissatisfaction or dissatisf$)	122	L12
L11	L10 and customer	5259	L11
L10	L3 amd credit near account	31265	L10
	DB=USPT; PLUR=YES; OP=OR		
L9	(5287268 | 5466919 | 5056019 | 5025372 | 5483444 | 5297026 | 5537314 | 5621640 | 5053957 | 5710886)![PN]	10	L9
L8	('6128599')[PN]	1	L8
L7	(6014661 | 5696907 | 6188988 | 5930764 | 6029153 | 6016477 | 6012051 | 5177684 | 6021397 | 6018718 | 6236975 | 5875236 | 5537590 | 6029149 | 6151565 | 5481647 | 5649116 | 6125359 | 6009420 | 6292787 | 6119103 | 6029138 | 5953704 | 5706406 | 6163604 | 6182060 | 5517405 | 6151582 |	40	L7

	5630127 | 6275818 | 6115691 | 5687322 | 6128599 | 5406477 | 5404292 | 5182793 | 6249775 | 6286005 | 5940816 | 5930762)![PN]		
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR		
L6	('6609120')[ABPN1,NRPN,PN,TBAN,WKU]	3	L6
	DB=USPT; PLUR=YES; OP=OR		
L5	'6286005'.pn.	1	L5
L4	'6292787'.pn.	1	L4
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR		
L3	6609120.pn.	3	L3
L2	5870456.pn.	2	L2
L1	5357563.pn.	2	L1

END OF SEARCH HISTORY